CHARACTERIZING CONGRUENCE PRESERVING FUNCTIONS Z/nZ → Z/mZ VIA RATIONAL POLYNOMIALS

Serge Grigorieff, Irene Guessarian, Patrick Cégielski

CHARACTERIZING CONGRUENCE PRESERVING FUNCTIONS $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ VIA RATIONAL POLYNOMIALS

Patrick CÉGIELSKI [1]
LACL, EA 4219, Université Paris-Est Créteil, France
IUT Sénart-Fontainebleau
cegielski@u-pec.fr

Serge GRIGORIEFF [1]
LIAFA, CNRS and Université Paris-Diderot, France
seg@liafa.univ-paris-diderot.fr

Irène GUESSARIAN [1] [2]
LIAFA, CNRS and Université Paris-Diderot, France
ig@liafa.univ-paris-diderot.fr

Received: , Revised: , Accepted: , Published:

Abstract

We introduce a basis of rational polynomial-like functions $P_0, \ldots, P_{n-1}$ for the free module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We then characterize the subfamily of congruence preserving functions as the set of linear combinations of the functions $lcm(k)\, P_k$ where $lcm(k)$ is the least common multiple of $2, \ldots, k$ (viewed in $\mathbb{Z}/m\mathbb{Z}$). As a consequence, when $n \geq m$, the number of such functions is independent of n.

1. Introduction

The notion of congruence preserving function on rings of residue classes was introduced in Chen [3] and studied in Bhargava [1].

Definition 1.1. *Let $m, n \geq 1$. A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is said to be* congruence preserving *if for all d dividing m*

$$\forall a, b \in \{0, \ldots, n-1\} \qquad a \equiv b \pmod{d} \implies f(a) \equiv f(b) \pmod{d} \qquad (1)$$

Remark 1.2. 1. If $n \in \{1, 2\}$ or $m = 1$ then every function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is trivially congruence preserving.

[1] Partially supported by TARMAC ANR agreement 12 BS02 007 01.
[2] Emeritus at UPMC Université Paris 6. Corresponding author

2. Observe that since d is assumed to divide m, equivalence modulo d is a congruence on $(\mathbb{Z}/m\mathbb{Z}, +, \times)$. However, since d is not supposed to divide n, equivalence modulo d may not be a congruence on $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Example 1.3. 1. For functions $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, condition (1) reduces to the conditions $f(3) \equiv f(0) \pmod 3$, $f(4) \equiv f(1) \pmod 3$, $f(5) \equiv f(2) \pmod 3$.
2. For functions $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$, condition (1) reduces to $f(2) \equiv f(0) \pmod 2$, $f(3) \equiv f(1) \pmod 2$, $f(4) \equiv f(0) \pmod 4$, $f(5) \equiv f(1) \pmod 4$.

In this paper, we characterize congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ using the following ingredients. We denote by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ that of nonnegative integers (including zero).

Definition 1.4. *The unary* lcm *function* $\mathbb{N} \to \mathbb{N}$ *maps* 0 *to* 1 *and* $k \geq 1$ *to the least common multiple of* $1, 2, \ldots, k$.

A natural way to associate to each map from $\mathbb{N}$ to $\mathbb{Z}$ a map from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ is to restrict F to $\{0, \cdots, n-1\}$ and take its values modulo m.

Definition 1.5. *To each map* $F : \mathbb{N} \to \mathbb{Z}$ *we associate the map* $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *defined by* $f = \pi_m \circ F \circ \iota_n$ *where* $\pi_m(x) = x \pmod m$ *and* $\iota_n(z)$ *is the least element of* $\pi_n^{-1}(z)$ *(belonging to* $\{0, \ldots, n-1\}$*). Thus diagram* (2) *commutes*

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{F} & \mathbb{Z} \\ {\scriptstyle \iota_n}\uparrow & & \downarrow{\scriptstyle \pi_m} \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/m\mathbb{Z} \end{array} \tag{2}$$

Applying Definition 1.5 to binomial coefficients $\binom{x}{k}$ we get a basis of the $\mathbb{Z}/m\mathbb{Z}$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Proposition 1.6. *Let* $P_k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *be associated to the* $\mathbb{N} \to \mathbb{N}$ *binomial function* $x \mapsto \binom{x}{k}$. *For every function* $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *there is a unique sequence* $(a_0, \ldots, a_{n-1})$ *of elements of* $\mathbb{Z}/m\mathbb{Z}$ *such that*

$$f \quad = \quad \sum_{k=0}^{k=n-1} a_k \, P_k \tag{3}$$

The family $\{P_0, \ldots, P_{n-1}\}$ *is thus a basis of the* $\mathbb{Z}/m\mathbb{Z}$*-module of functions* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Our main result (Theorem 1.7) can be stated as

Theorem 1.7. *A function* $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *is congruence preserving if and only if, for each* $k = 0, \ldots, n-1$, *in equation* (3) *the coefficient* a_k *is a multiple of the residue of* $lcm(k)$ *in* $\mathbb{Z}/m\mathbb{Z}$.

The paper is organized as follows.

Proposition 1.6 is proved in Section 2 where, after recalling Chen's notion of polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ (cf. [3, 4]), we extend it to a notion of rational polynomial function.

The proof of our main result Theorem 1.7 is given in Section 3. We adapt the techniques of our paper [2], exploiting similarities between Definition 1.1 and the condition studied in [2] for functions $f : \mathbb{N} \to \mathbb{Z}$ (namely, $x-y$ divides $f(x)-f(y)$ for all $x, y \in \mathbb{N}$). As a consequence of Theorem 1.7 the number of congruence preserving functions is independent of n for $n \geq m$ and even for $n \geq gpp(m)$ (the greatest prime power dividing m). Also, every congruence preserving function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is rational polynomial for a polynomial of degree strictly less than the minimum between n and $gpp(m)$.

In Section 4 we use our main theorem to count the congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We thus get an expression equivalent to that obtained by Bhargava in [1] and which makes apparent the fact that, for $n \geq gpp(m)$ (hence for $n \geq m$), this number depends only on m and is independent of n.

2. Representing functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by rational polynomials

In [3, 1], congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are introduced and studied together with an original notion of polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Definition 2.1 (Chen [3])**.** *A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is* polynomial *if it is associated (in the sense of Definition 1.5) to a function $F : \mathbb{N} \to \mathbb{Z}$ given by a polynomial in $\mathbb{Z}[X]$.*

Polynomial functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are obviously congruence preserving. Are all congruence preserving functions polynomial? Chen [3] observe that it is not the case for some values of n, m, for instance $n = 6$, $m = 8$. He also proves that a stronger identity holds for infinitely many pairs (n, m) : *every function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is polynomial if and only n is not greater than the first prime factor of m.* Using counting arguments, Bhargava [1] characterizes the pairs (n, m) such that every congruence preserving function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is polynomial.

Some polynomials in $\mathbb{Q}[X]$ (i.e. polynomials with rational coefficients) happen to map integers into integers.

Definition 2.2. *For $k \in \mathbb{N}$, let $P_k \in \mathbb{Q}[X]$ be the following polynomial:*

$$P_k(x) = \binom{x}{k} = \frac{\prod_{i=0}^{k-1}(x-i)}{k!}.$$

We will use the following examples later on:

$P_0(x) = 1$, $P_1(x) = x$, $P_2(x) = x(x-1)/2$, $P_3(x) = x(x-1)(x-2)/6$, $P_4(x) = x(x-1)(x-2)(x-3)/24$, $P_5(x) = x(x-1)(x-2)(x-3)(x-4)/120$.

In [5] (1915), Pólya used the P_k to give the following very elegant and elementary characterization of polynomials in $\mathbb{Q}[X]$ mapping integers to integers.

Theorem 2.3 (Pólya)**.** *A polynomial in $\mathbb{Q}[X]$ is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials P_k.*

It turns out that the representation of functions $\mathbb{N} \to \mathbb{Z}$ as $\mathbb{Z}$-linear combinations of the P_k's used in [2] also fits in the case of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$: every such function is a $(\mathbb{Z}/m\mathbb{Z})$-linear combination of the P_k's.

Definition 2.4. *A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is* rat-polynomial *if is associated in the sense of Definition 1.5 with some polynomial in $\mathbb{Q}[X]$. The degree of f is the smallest among the degrees of such polynomials.*

We denote by $P_k^{n,m}$ the rat-polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ associated with the polynomial P_k of Definition 2.2 in the sense of Definition 1.5. When there is no ambiguity, $P_k^{n,m}$ will be denoted simply as P_k.

Remark 2.5. In Definition 2.4, the polynomial *crucially depends* on the choice of representatives of elements of $\mathbb{Z}/n\mathbb{Z}$: e.g. for $n = m = 6$, $0 \equiv 6 \pmod 6$ but $0 = P_2(0) \not\equiv P_2(6) = 3 \pmod 6$. The chosen representatives for elements of $\mathbb{Z}/n\mathbb{Z}$ will always be $\{0, \dots, n-1\}$.

We now prove the representation result by the P_k's.

Proof of Proposition 1.6. Let us start with uniqueness. We have $f(0) = a_0$ hence the first coefficient a_0 is $f(0)$. We have $f(1) = a_0 + a_1$, hence $a_1 = f(1) - f(0)$. By induction, and noting that $P_k(k) = 1$, we have $f(k) = Q(k) + a_k.P_k(k) = Q(k) + a_k$, hence we are able determine a_k.

For existence, argue backwards to see that this sequence suits. □

Remark 2.6. The evaluation of $a_k\, P_k(x)$ in $\mathbb{Z}/m\mathbb{Z}$ has to be done as follows: for x an element of $\mathbb{Z}/n\mathbb{Z}$, we consider it as an element of $\{0, \dots, n-1\} \subseteq \mathbb{N}$ and we evaluate $P_k(x) = \dfrac{1}{k!} \prod_{i=0}^{k-1} (x-i)$ as an element of $\mathbb{N}$, then we consider the remainder modulo m, and finally we multiply the result by a_k in $\mathbb{Z}/m\mathbb{Z}$. For instance, for $n = m = 8$, $4\, P_2(3) = 4 \times \dfrac{3 \times 2}{2} = 4 \times 3 = 4$, but we might be tempted to evaluate it as $4\, P_2(3) = \dfrac{4 \times 3 \times 2}{2} = \dfrac{0}{2} = 0$, which does **not** correspond to our definition. However, dividing a_k by a factor of the denominator is allowed.

Corollary 2.7. *(1) Every function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is rat-polynomial with degree less than n.*
(2) The family of rat-polynomial functions $(P_k)_{k=0,\dots,n-1}$ is a basis of the $(\mathbb{Z}/m\mathbb{Z})$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Example 2.8. The function $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ defined by

$0 \mapsto 0 \quad 1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 3 \quad 4 \mapsto 0 \quad 5 \mapsto 1$

is represented by the rational polynomial $P_f(x) = 3x + 4\frac{x(x-1)}{2}$ which can be simplified into $P_f(x) = 3x - x(x-1)$ on $\mathbb{Z}/6\mathbb{Z}$.

Example 2.9. The function $f\colon \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/8\mathbb{Z}$ given by Chen [3] as a non polynomial congruence preserving function, namely the function defined by $f(0) = 0\ ,\ f(1) = 3\ ,\ f(2) = 4\ ,\ f(3) = 1\ ,\ f(4) = 4\ ,\ f(5) = 7$, is represented by the rational polynomial with coefficients $a_0 = 0\,,\ a_1 = 3\,,\ a_2 = 6\,,\ a_3 = 2\,,\ a_4 = 4\,,\ a_5 = 4$, i.e.

$$\begin{aligned} f(x) &= 3x + 6\frac{x(x-1)}{2} + 2\frac{x(x-1)(x-2)}{2} + 4\ \frac{x(x-1)(x-2)(x-3)}{8} \\ &\quad +4\ \frac{x(x-1)(x-2)(x-3)(x-4)}{8} \\ &= 3x + 3x(x-1) + x(x-1)(x-2) + \ \frac{x(x-1)(x-2)(x-3)}{2} \\ &\quad + \ \frac{x(x-1)(x-2)(x-3)(x-4)}{2}\,. \end{aligned}$$

3. Characterizing congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Congruence preserving functions $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ can be characterized by a simple condition on the coefficients of the rat-polynomial representation of f given in Proposition 1.6.

3.1. Proof of Theorem 1.7

For proving Theorem 1.7 we will need some relations involving binomial coefficients and the unary *lcm* function; these relations are stated in the next three lemmata. The proofs are elementary but technical and can be found in our paper [2].

Lemma 3.1. *If* $0 \le n-k < p \le n < m$ *then* p *divides* $lcm(k)\binom{n}{k}$.

Lemma 3.2. *If* $n, k, b \in \{0, 1, \ldots, m-1\}$ *and* $k \le b$ *then* n *divides* $A^n_{k,b} = lcm(k)\left(\binom{b+n}{k} - \binom{b}{k}\right)$.

The following is an immediate consequence of Lemma 3.2 (set $a = b + n$).

Lemma 3.3. *If* $m > a \ge b$ *then* $a - b$ *divides* $lcm(k)\left(\binom{a}{k} - \binom{b}{k}\right)$ *for all* $k \le b$.

Besides these lemmata, we shall use a classical result in $\mathbb{Z}/m\mathbb{Z}$. For $x, y \in \mathbb{Z}$ we say *x divides y in $\mathbb{Z}/m\mathbb{Z}$* if and only if the residue class of x divides the residue class of y in $\mathbb{Z}/m\mathbb{Z}$.

Lemma 3.4. *Let $a_1, \ldots, a_k \geq 1$ and c be their least common multiple. If $a_1, \ldots, a_k$ all divide x in $\mathbb{Z}/m\mathbb{Z}$ then so does c.*

Proof. It suffices to consider the case $k = 2$ since the passage to any k is done via a straightforward induction. Let $c = a_1 b_1 = a_2 b_2$ with b_1, b_2 coprime. Let t, u be such that $x = a_1 t = a_2 u$ in $\mathbb{Z}/m\mathbb{Z}$. Then $x \equiv a_1 t \equiv a_2 u \pmod{m}$. Using Bézout identity, let $\alpha, \beta \in \mathbb{Z}$ be such that $\alpha b_1 + \beta b_2 = 1$. Then

$$c(t\alpha + u\beta) \;=\; a_1 b_1 t\alpha + a_2 b_2 u\beta \;\overset{\text{mod } m}{\equiv}\; x\alpha b_1 + x\beta b_2 \;=\; x$$

hence $c(t\alpha + u\beta) = x$, proving that c divides x in $\mathbb{Z}/m\mathbb{Z}$. □

Proof of Theorem 1.7. "Only if" part. Assume $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving and consider its decomposition $f(x) = \sum_{k=0}^{n-1} a_k P_k^{n,m}(x)$ given by Proposition 1.6. We show that $lcm(k)$ divides a_k in $\mathbb{Z}/m\mathbb{Z}$ for all $k < n$.

Claim 1. *For all $m > k \geq 1$, k divides a_k.*

Proof. By induction on k. Recall that $f(k) = a_i \sum_{i=0}^{n-1} \binom{k}{i} = a_i \sum_{i=0}^{k} \binom{k}{i}$ by noting that $\binom{k}{i} = 0$ for $i > k$.
Induction Basis: The case $k = 1$ is trivial. For $k = 2$, if 2 does not divide m then 2 is invertible in $\mathbb{Z}/m\mathbb{Z}$, hence 2 divides a_2. Otherwise, observe that, as 2 divides $2 - 0$, and f is congruence preserving, 2 divides $f(2) - f(0) = 2a_1 + a_2$ hence 2 divides a_2.
Induction: assuming that ℓ divides a_ℓ for every $\ell \leq k$, we prove that $k + 1$ divides a_{k+1}. Assume first that $k + 1$ divides m, then

$$\begin{aligned} f(k+1) - f(0) &= (k+1)a_1 + \left(\sum_{i=2}^{k} \binom{k+1}{i} a_i \right) + a_{k+1} \\ &= (k+1)a_1 + \left(\sum_{i=2}^{k} (k+1)\, \frac{a_i}{i} \binom{k}{i-1} \right) + a_{k+1}\,. \end{aligned} \tag{4}$$

By the induction hypothesis, $\dfrac{a_i}{i}$ is an integer for $i \leq k$. Since f is congruence preserving, $k + 1$ divides $f(k + 1) - f(0)$ hence $k + 1$ divides the last term a_{k+1} of the sum.

Assume now that $k + 1$ does not divide m, then $k + 1 = a \times b$ with b dividing m and a coprime with m. Hence a is invertible in $\mathbb{Z}/m\mathbb{Z}$ and, by the congruence preservation property of f, b divides $f(k + 1) - f(0)$; as b divides $k + 1$, equation (4) implies that b divides a_{k+1}, and $a \times b$ also divides a_{k+1} (by invertibility of a and Lemma 3.4). □

Claim 2. *For all $1 \leq p \leq k$, p divides a_k. Thus, $lcm(k)$ divides a_k in $\mathbb{Z}/m\mathbb{Z}$.*

Proof. The last assertion of Claim 2 is a direct application of Lemma 3.4 to the first assertion which we now prove. The case $p = 1$ is trivial. We prove the case $p \geq 2$ by induction on p.

• *Basic case $p = 2$: 2 divides a_k for all $k \geq 2$.* If 2 does not divide m, then 2 is invertible and divides all numbers in $\mathbb{Z}/m\mathbb{Z}$; assume that 2 divides m. We argue by induction on $k \geq 2$.

- *Basis.* Apply Claim 1: 2 divides a_2.

- *Induction.* Assuming that 2 divides a_i for all $2 \leq i \leq k$ we prove that 2 divides a_{k+1}. Two cases can occur.

Subcase 1: $k+1$ is odd. Then, k is even, 2 divides k and, by congruence preservation, 2 divides $f(k+1) - f(1)$. We have

$$f(k+1) - f(1) = ka_1 + \left(\sum_{i=2}^{k} a_i \tbinom{k+1}{i}\right) + a_{k+1},$$

2 divides the a_i for $2 \leq i \leq k$ by the induction hypothesis, 2 also divides k, hence, 2 divides a_{k+1}.

Subcase 2: $k+1$ is even. Then 2 divides $f(k+1) - f(0)$. Now,

$$f(k+1) - f(0) = (k+1)a_1 + \left(\sum_{i=2}^{k} a_i \tbinom{k+1}{i}\right) + a_{k+1},$$

$k+1$ is even and 2 divides the a_i for $2 \leq i \leq k$ by the induction hypothesis, thus, 2 divides a_{k+1}.

• *Induction step: $p \geq 2$ and $p+1 < n$. Assume that*

$$\textit{for all } q \leq p \ , \ q \textit{ divides } a_\ell \ \textit{ for all } \ \ell \ \textit{ such that } q \leq \ell < n \tag{5}$$

and prove that $p+1$ divides a_k for all k such that $p+1 \leq k < n$. Again, we use induction on $k \geq p+1$ and we assume that k divides m in order to use congruence preservation. When k does not divide m we factorize it as $k = ab$ with b dividing m and a coprime with m and a similar proof will show that b divides a_k and k divides a_k (cf. the proof of Induction in Claim 1).

- *Basis $k = p+1$.* Follows from Claim 1: $p+1$ divides a_{p+1}.

- *Induction.* Assuming that $p+1$ divides a_i for all i such that $p+1 \leq i \leq k$, we prove that $p+1$ divides a_{k+1}. As $p+1$ divides $k+1-(k-p)$ and f is congruence preserving, $p+1$ divides $f(k+1) - f(k-p)$ which is given by

$$f(k+1) - f(k-p) = \sum_{i=1}^{k-p} a_i \left(\binom{k+1}{i} - \binom{k-p}{i} \right) + \left(\sum_{i=k+1-p}^{k} a_i \binom{k+1}{i} \right) + a_{k+1}\,. \tag{6}$$

First look at the terms of the first sum corresponding to $1 \leq i \leq p$. The induction

hypothesis (5) on p implies that q divides a_k for all $q \leq p$ and $k \geq q$. In particular, letting $k = i$ and using Lemma 3.4, we see that $lcm(i)$ divides a_i in $\mathbb{Z}/m\mathbb{Z}$. As $(k+1)-(k-p) = p+1$, by Lemma 3.2 we have: $p+1$ divides $lcm(i)\left(\binom{k+1}{i} - \binom{k-p}{i}\right)$. A fortiori, $p+1$ divides $a_i\left(\binom{k+1}{i} - \binom{k-p}{i}\right)$.

We now turn to the terms of the first sum corresponding to $p+1 \leq i \leq k-p$ (if there are any). Again by the induction hypothesis (on k), $p+1$ divides a_i for all $p+1 \leq i \leq k$. Thus, each term of the first sum is divisible by $p+1$.

Consider now the terms of the second sum. By the induction hypothesis (on k), $p+1$ divides a_i for all $p+1 \leq i \leq k$. It remains to look at the terms associated with the i's such that $k+1-p \leq i \leq p$ (there are such i's in case $k+1-p < p+1$). For such i's we have $0 \leq (k+1) - i \leq (k+1) - p < p+1 \leq k+1$ and Lemma 3.1 (used with $k+1, i$ and $p+1$ in place of n, k and p) insures that $p+1$ divides $lcm(i)\binom{k+1}{i}$. Now, for such i's, the induction hypothesis (5) on p shows that $lcm(i)$ divides a_i. Thus, $p+1$ divides each $a_i\binom{k+1}{i}$.

As $p+1$ divides the k first terms of the right-hand side of (6) and also divides the left-hand side, it must divide the last term a_{k+1} of the right-hand side. This ends the proof of the induction in the inductive step hence also the proof of Claim 2, and of the "only if" part of the Theorem. □

"If" part of Theorem 1.7. Assuming all the a_k's in equation (3) are divisible by $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$ we prove that f is congruence preserving, i.e. that, for all $a, b \in \{0, \ldots, n-1\}$, if $a-b$ divides n then $a-b$ divides $f(a)-f(b)$ in $\mathbb{Z}/m\mathbb{Z}$.

If all the a_k's in equation (3) are divisible by $lcm(k)$ then f can be written in the form $f(n) = \sum_{k=0}^{n} b_k lcm(k)\binom{n}{k}$. Consequently,

$$f(a) - f(b) = \left(\sum_{k=0}^{b} b_k lcm(k)\left(\binom{a}{k} - \binom{b}{k}\right)\right) + \sum_{k=b+1}^{a} b_k lcm(k)\binom{a}{k}.$$

By Lemma 3.3, $a-b$ divides each term of the first sum.

Consider the terms of the second sum. For $b+1 \leq k \leq a$, we have $0 \leq a-k < a-b \leq a$ and Lemma 3.1 (used with a, k and $a-b$ in place of n, k and p) insures that $a-b$ divides $lcm(k)\binom{a}{k}$. Hence, $a-b$ divides each term of the second sum. □

3.2. On a family of generators

We now sharpen the degree of the rat-polynomial representing a congruence preserving function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We need first some properties of the lcm function and a definition.

Lemma 3.5. *In $\mathbb{Z}/m\mathbb{Z}$ we have $lcm(k) = u \times \prod p_i^{\alpha_i^k}$ with u invertible in $\mathbb{Z}/m\mathbb{Z}$, p_i prime and dividing m, and $\alpha_i^k = \max\{\beta_i | p_i^{\beta_i} \leq k\}$.*

Definition 3.6. *For $m \geq 1$, with prime factorization $m = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$, let $gpp(m) = \max_{i=1,\ldots,\ell} p_i^{\alpha_i}$ be the greatest power of prime dividing m.*

Example 3.7. In $\mathbb{Z}/m\mathbb{Z}$ the element $lcm(k)$ is zero for k large enough.

In $\mathbb{Z}/8\mathbb{Z}$

k	1	2	3	4	5	6	7	8
$lcm(k)$	1	2	2	4	4	4	4	0

$gpp(8) = 8$

In $\mathbb{Z}/12\mathbb{Z}$

k	1	2	3	4	5	6	7	8	9	10	11
$lcm(k)$	1	2	6	0	0	0	0	0	0	0	0

$gpp(12) = 4$

Lemma 3.8. *The number $gpp(m)$ is the least integer k such that $lcm(k)$ is zero in $\mathbb{Z}/m\mathbb{Z}$. Moreover for all $\ell \geq gpp(m)$, $lcm(\ell)$ is zero in $\mathbb{Z}/m\mathbb{Z}$.*

Remark 3.9. (1) Either $gpp(m) = m$ or $gpp(m) \leq m/2$.
(2) In general, $gpp(m)$ is greater than $\lambda(m)$, the least k such that m divides $k!$ considered in [3]: for $m = 8$, $gpp(m) = 8$ whilst $\lambda(m) = 4$.

Using Lemma 3.8, we can get a better version of Theorem 1.7.

Theorem 3.10. *A function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving if and only if it is associated in the sense of Definition 1.5 with a rational polynomial $P = \sum_{k=0}^{d-1} a_k \binom{x}{k}$ where $d = \min(n, gpp(m))$ and such that $lcm(k)$ divides a_k in $\mathbb{Z}/m\mathbb{Z}$ for all $k < d$.*

Proof. For $k \geq gpp(m)$, m divides $lcm(k)$ hence the coefficient a_k is 0. □

Theorem 3.11. *(1) Every congruence preserving function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is rat-polynomial with degree less than $gpp(m)$.*
(2) The family of rat-polynomial functions

$$\mathcal{F} = \{lcm(k)(P_k^{n,m}) | 0 \leq k < \min(n, gpp(m))\}$$

generates the set of congruence preserving functions.
(3) $\mathcal{F}$ is a basis of the set of congruence preserving functions if and only if m has no prime divisor $p < \min(n, m)$ (in case $n \geq m$ this means that m is prime) .

Proof. (1) and (2) are restatements of Theorem 3.10 . We prove (3).
"Only If" part. Asssuming m has a prime divisor $p < \min(n, m)$, let p be the least one. Then $\mathcal{F}$ is not linearly independent. In $\mathbb{Z}/m\mathbb{Z}$, $lcm(p) \neq 0$ hence $lcm(p)\, P_p^{n,m}$ is not the null function since $P_p^{n,m}(p) = 1$. However $(m/p)\, lcm(p) = 0$ hence $(m/p)\, lcm(p)\, P_p^{n,m}$ is the null function. As $(m/p) \neq 0$, we see that $\mathcal{F}$ cannot be a basis.
"If" part. Assume that m has no prime divisor $p < \min(n, m)$. We prove that $\mathcal{F}$

is $\mathbb{Z}/m\mathbb{Z}$-linearly independent. Suppose that the $\mathbb{Z}/m\mathbb{Z}$-linear combination $L = \sum_{k=0}^{\min(n,gpp(m))-1} a_k\, lcm(k)\, P_k^{n,m}$ is the null function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. By induction on $k = 0, \ldots, \min(n, gpp(m)) - 1$ we prove that $a_k = 0$.

• *Basic cases* $k = 0, 1$. Since $L(0) = a_0$ we get $a_0 = 0$. Since $L(1) = a_0 + a_1 1$ we get $a_1 = 0$.

• *Induction step.* Assuming that $k \geq 2$ and $a_i = 0$ for $i = 0, \ldots, k-1$, we prove that $a_k = 0$. Note that $P_\ell^{n,m}(k) = \binom{k}{\ell}$ for $k < \ell < n$. Since $a_i = 0$ for $i = 0, \ldots, k-1$, and $P_k^{n,m}(k) = 1$ we get $L(k) = a_k\, lcm(k)$. Since $k < \min(n, gpp(m))$ and m has no prime divisor $p < \min(n, m)$, the numbers $lcm(k)$ and m are coprime hence $lcm(k)$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ and equality $L(k) = a_k lcm(k) = 0$ implies $a_k = 0$. □

4. Counting congruence preserving functions

We are now interested in the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. As two different rational polynomials correspond to different functions by Proposition 1.6 (uniqueness of the representation by a rational polynomial), the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is equal to the number of polynomials representing them.

Proposition 4.1. *Let $CP(n, m)$ be the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. For $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$, we have*

$$CP(n,m) = p_1^{p_1+p_1^2+\cdots+p_1^{e_1}} \times \cdots \times p_\ell^{p_\ell+p_\ell^2+\cdots+p_\ell^{e_\ell}} \quad \text{if } n \geq gpp(m), \text{ and}$$

$$CP(n,m) = \prod_{\{i|p_i^{e_i} < gpp(m)\}} p_i^{p_i+p_i^2+\cdots+p_i^{e_i}} \times \prod_{\{i|p_i^{e_i} \geq gpp(m)\}} p_i^{p_i+p_i^2+\cdots+p_i^{\lfloor \log_p n \rfloor}+n(e-\lfloor \log_p n \rfloor)}$$
$$\text{if } n < gpp(m).$$

Equivalently, using an à la Vinogradov's notation for better readability and writing $E(p, \alpha)$ in place of p^α we have

$$CP(n,m) = \prod_{i=1}^{\ell} E(p_i, \sum_{k=1}^{e_i} p_i^k) \quad \text{if } n \geq gpp(m), \text{ and}$$

$$CP(n,m) = \prod_{\{i|p_i^{e_i} < gpp(m)\}} E(p_i, \sum_{k=1}^{e_i} p_i^k) \times \prod_{\{i|p_i^{e_i} \geq gpp(m)\}} E(p_i, \sum_{k=1}^{\lfloor \log_p n \rfloor} p_i^k + n(e - \lfloor \log_p n \rfloor))$$
$$\text{if } n < gpp(m).$$

Corollary 4.2. *For $n \geq gpp(m)$, $CP(n, m)$ does* not *depend on n.*

Proof of Proposition 4.1. By Theorem 3.10, we must count the number of n-tuples of coefficients $(a_0, \ldots, a_{n-1})$, with a_k a multiple of $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$.

Claim 1. *For $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$, for all n, $CP(n,m) = \Pi_{i=1}^{i=\ell}\ CP(n, p_i^{e_i})$.*

Proof. Let $\lambda(m,k)$ be the number of multiples of $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$, i.e. order of the subgroup generated by $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$.

Since $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\Pi_{i=1}^{i=\ell}\mathbb{Z}/p_i^{e_i}\mathbb{Z}$, we have $\lambda(m,k) = \Pi_{i=1}^{i=\ell}\lambda(p_i^{e_i},k)$ for each k. Thus, the number of n-tuples $(a_0,\ldots,a_{n-1})$ such that $lcm(k)$ divides a_k is equal to

$$\Pi_{k<n}\lambda(m,k) = \Pi_{k<n}\ \Pi_{i=1}^{i=\ell}\lambda(p_i^{e_i},k) = \Pi_{i=1}^{i=\ell}\ \Pi_{k<n}\lambda(p_i^{e_i},k)\,.$$

The trick in the proof is the permutation of the two products; hence the Claim by using Theorem 1.7. □

Claim 1 reduces the problem to counting the congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. We will now use Proposition 3.10 for this counting.

Claim 2.

$$CP(n,p^e) = \begin{cases} p^{p+p^2+\cdots+p^e} & \text{if } n \geq p^e \\ p^{p+p^2+\cdots+p^l+(e-l)n} & \text{if } p^l \leq n < p^e \text{with } l = \lfloor \log_p n \rfloor. \end{cases}$$

Proof. By Theorem 3.10, as $gpp(p^e) = p^e$, letting $\nu = \inf(n,p^e)$, $CP(n,p^e) = CP(\nu,p^e) = \Pi_{k<\nu}\lambda(p^e,k)$. For $p^j \leq k < p^{j+1}$ the order $\lambda(p^e,k)$ of the subgroup generated by $lcm(k)$ in $\mathbb{Z}/p^e\mathbb{Z}$ is p^{e-j} and there are $p^{j+1}-p^j$ such k's.
• Assume first $n \geq p^e$, then $CP(n,p^e) = CP(p^e,p^e) = p^M$ with

$$\begin{aligned} M &= ep + (e-1)(p^2-p) + \cdots + (e-j)(p^{j+1}-p^j) + \cdots + p^e - p^{e-1} \\ &= ep + \sum_{j=1}^{e-1}(e-j)(p^{j+1}-p^j) = p + p^2 + \cdots + p^e\,. \end{aligned}$$

• Assume then $p^l \leq n < p^e$, with $l = \lfloor \log_p n \rfloor$; then $CP(n,p^e) = p^M$ with

$$\begin{aligned} M &= ep + \sum_{j=1}^{l-1}(e-j)(p^{j+1}-p^j) + (e-l)(n-p^l) \\ &= p + p^2 + \cdots + p^l + n(e-l)\,. \end{aligned}$$

□

This finishes the proof of Proposition 4.1. □

Remark 4.3. In [1] the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$ is shown to be equal to $p^{en-\sum_{k=1}^{n-1}\min\{e,\lfloor\log_p k\rfloor\}}$. For $p^i \leq k < p^{i+1}$, $\lfloor \log_p k \rfloor = i$, hence: for $k \leq p^e$, $\min\{e, \lfloor \log_p k \rfloor\} = \lfloor \log_p k \rfloor$ and for $k \geq p^e$, $\min\{e, \lfloor \log_p k \rfloor\} = e$.

We thus have
• if $n \geq p^e$,

$$\begin{aligned} \sum_{k=1}^{n-1} \min\{e, \lfloor \log_p k \rfloor\} &= \sum_{k=1}^{p^e-1} \lfloor \log_p k \rfloor + \sum_{k=p^e}^{n-1} e \\ &= \sum_{j=0}^{e-1} j(p^{j+1} - p^j) + e(n - p^e) \\ &= -(p + \cdots + p^e) + ep^e + e(n - p^e) \end{aligned}$$

$$\text{hence} \qquad en - \sum_{k=1}^{n-1} \min\{e, \lfloor \log_p k \rfloor\} = p + \cdots + p^e$$

$$\text{and} \qquad p^{en - \sum_{k=1}^{n-1} \min\{e, \lfloor \log_p k \rfloor}} = p^{p+p^2+\cdots+p^e}$$

which coincides with our counting in Claim 2.

• if $n < p^e$, and $l = \lfloor \log_p n \rfloor$, then similarly

$$\begin{aligned} \sum_{k=1}^{n-1} \lfloor \log_p k \rfloor &= \sum_{k=1}^{l-1} \lfloor \log_p k \rfloor + \sum_{k=l}^{n-1} \lfloor \log_p k \rfloor \\ &= \sum_{j=0}^{l-1} j(p^{j+1} - p^j) + l(n - p^l) = -(p + \cdots + p^l) + nl \end{aligned}$$

and $en - \sum_{k=1}^{n-1} \lfloor \log_p k \rfloor = p + \cdots + p^l + (e - l)n$, which again coincides with our counting in Claim 2.

5. Conclusion

We proved that the rational polynomials $lcm(k)\, P_k^{n,m}$ generate the $(\mathbb{Z}/m\mathbb{Z})$-submodule of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. When n is larger than the greatest prime power dividing m, the number of functions in this submodule is independent of n. An open problem is the existence of a basis of this submodule.

Acknowledgments : We are extremely grateful to the anonymous referee for his insightful reading and valuable comments which helped improving the readability of the paper.

References

[1] M. Bhargava, *Congruence preservation and polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Discrete Mathematics 173 (1997), p. 15 – 21.

[2] P. Cégielski, S. Grigorieff, I. Guessarian, *Newton expansion of functions over natural integers having integral difference ratios*, Int. J. Number Theory, Vol. 11 No 7 (2015), p. 2109-2139.

[3] Z. Chen, *On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Discrete Math. 137 (1995), p. 137–145.

[4] Z. Chen, *On polynomial functions from* $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ *to* $\mathbb{Z}_m$, Discrete Math. 162 (1996), p. 67–76.

[5] G. Pólya, *Über ganzwertige ganze Funktionen*, Rend. Circ. Mat. Palermo 40 (1915), p. 1–16.